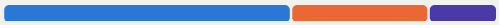
Cyber Watch

2026-W43 · 19 Oct – 25 Oct 2026
Makani Lab · Cyber Watch
Operations · Force Protection · Professionals

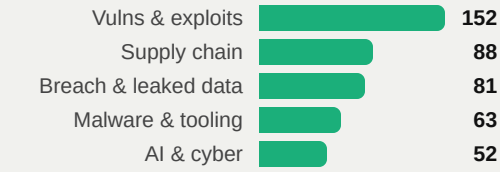
BLUF — PRC actor Storm-0940 used AI agents to breach 2,250+ M365 tenants via ConnectWise; SafePay and PHP2Shell hit edge and web systems. Needs attention: Arista and Collabora KEV due 26 Oct.

LAST 7 DAYS BY LANE · 381 ITEMS

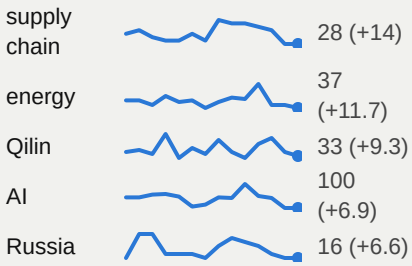


Operations 222 · Force Protection 106 · Space & Cyber Professionals 53

CATEGORIES



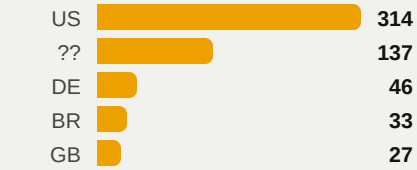
RISING TERMS · 7D VS PRIOR



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 8 (0 ransomware-linked) · leak-site victims 187 (76 PACOM AOR)

LEAK-SITE VICTIMS BY COUNTRY · 30D



THREAT ACTOR SPOTLIGHT — STORM-0940 · PRC (state-aligned, per Microsoft)

WHY NOW
Microsoft tied the ConnectWise breach to Storm-0940 using ARTEX AI agents.

MENTIONS, 30D



5 this week

PACOM RELEVANCE
Targets defense and military M365 tenants.

NOTABLE TTPS
- Password spraying at 2,900 attempts/min
- OAuth app abuse; AI-automated privilege changes

COUNTERMEASURES
- Review service-principal sign-ins and OAuth consents
- Enforce MFA and lockout

Operations

Threats to networks, missions, and infrastructure the command depends on: exploited vulns, intrusions, APT campaigns, ICS/OT, SATCOM/PNT, telecom.

#StopRansomware: SafePay Ransomware

CISA Cybersecurity Advisories · 2026-10-20

CISA/FBI: SafePay has hit 600+ organizations via stolen passwords, phishing and Cisco ASA/FTD flaws.

So what: Partner VPNs and firewalls are the way in.

Consider: Consider confirming VPN MFA and ASA/FTD patches.

PACOM · NORTHCOM · Ransomware · Critical infrastructure

US agencies urge fixes for programming language flaws putting millions of web systems at risk

Nextgov/FCW — cybersecurity · 2026-10-21

CISA urged immediate patching of PHP2Shell RCE; Amazon says exploitation began before the 21 Oct fix.

So what: PHP hides inside many appliances.

Consider: Recommend inventorying internet-facing PHP.

NORTHCOM · EUCOM · Vulns & exploits · Critical infrastructure

KEV: CVE-2026-114625 — Arista VeloCloud Orchestrator

CISA Known Exploited Vulnerabilities · 2026-10-22

KEV: exploited Arista VeloCloud Orchestrator SQLi and Collabora/Nextcloud RCE, both due 26 Oct.

So what: An SD-WAN orchestrator controls every site.

Consider: Recommend confirming fixed versions.

CYBERCOM · Vulns & exploits

Force Protection

What Guardians, Airmen, civilians, and families need to know personally: scams, social engineering, apps and devices, OPSEC, breaches of consumer services, official guidance.

Philippines-Based American Fraudster Pleads Guilty to Targeting Thousands of U.S. Servicemembers and Veterans

Department of Justice press releases · 2026-10-20

Boling pleaded guilty to using stolen PII of thousands of servicemembers and veterans to drain accounts.

So what: The data came from an Army records contractor in Korea.

Consider: Consider credit freezes for members and families.

PACOM · Scams & fraud · Breach & leaked data

Chinese National Extradited for Alleged Role in Multimillion-Dollar Cryptocurrency Scam Targeting U.S. Citizens

Department of Justice press releases · 2026-10-23

A Chinese national was arraigned for a Cambodia-run crypto investment scam targeting Americans.

So what: Scam centers keep targeting U.S. persons.

Consider: Be aware of unsolicited investment contacts.

PACOM · Scams & fraud · Social engineering · SE Asia scam compounds

DHS to ban DeepSeek from federal civilian agencies

CyberScoop · 2026-10-19

DHS barred DeepSeek from federal civilian agencies, citing data stored in China.

So what: The risk carries over to personal devices.

Consider: Be aware that prompts may reach the PRC.

NORTHCOM · Apps & devices · Policy & guidance

Space & Cyber Professionals

Context for the cyber and space workforce: strategy, doctrine, policy, organization, workforce, standards, exercises, industry and technology trends.

Space Force aims to beef up guardian presence for Centcom and other combatant commands

DefenseScoop · 2026-10-20

CSO Gen. Schiess called for Guardians 'at scale' at combatant commands.

So what: Components carry that presence.

Consider: Consider how SPACEPAC cyber billets fit.

SPACECOM · PACOM · Strategy & organization · Workforce & training · Scattered Spider

Managing AI Token Consumption for Operational Resilience

CISA Cybersecurity Advisories · 2026-10-22

CISA and partners issued guidance on AI token exhaustion and denial-of-wallet risk.

So what: AI-dependent workflows need fallbacks.

Consider: Recommend reviewing before fielding AI.

CYBERCOM · Policy & guidance · AI & cyber

Singapore’s CSA and Google identify safeguards and access controls to address autonomous AI agent risks

Industrial Cyber · 2026-10-21

Singapore's CSA and Google ran an agentic-AI tabletop urging runtime guardrails and agent identity.

So what: A regional partner is shaping AI-agent norms.

Consider: Be aware when setting theater AI requirements.

PACOM · AI & cyber · Standards & compliance

WATCH LIST

- Arista and Collabora KEV due 26 Oct.
- Siemens and Plex KEV due 3 Nov.
- Unpatched PHP RCE (mitigation only).
- n0n maritime extortion via CyberLogitec (ROK).

RECOMMENDATIONS (FOR AWARENESS)

- Recommend closing the 26 Oct KEV entries.
- Consider reviewing OAuth app consents.
- Consider a family note on credit freezes and scams.